ERDC/CRREL TR-05-11

Cold Regions Research and Engineering Laboratory

US Army Corps of Engineers®
Engineer Research and Development Center

Technology for Range Security

Lindamae Peck

June 2005

ERDC/CRREL TR-05-11
June 2005

Technology for Range Security

Lindamae Peck

U.S. Army Engineer Research and Development Center
Cold Regions Research and Engineering Laboratory
72 Lyme Road
Hanover NH 03755-1290

Prepared for U.S. Army Environmental Center
Aberdeen Proving Ground, MD 21010-5401

ABSTRACT: Commercial security equipment can support all the scenarios for monitoring training lands that are outlined in the sections, *Security options* and *Discrimination between humans and animals*. Specific products in the categories of intrusion detection systems, automated video surveillance, cameras, and illuminators are represented in a database of security technology. The database is a mix of current versions of long established security equipment and new, innovative technology. The variety of equipment means that there are many options for monitoring access at training lands without constraining military use of the sites. The Security Technology Decision Tree Tool (STDTT) assists a user unfamiliar with security technology in defining his site-specific security objectives, developing surveillance options, and selecting suitable equipment. STDTT operates on the security technology database to extract products that match the requirements developed from the user's decisions as he or she proceeds through the decision tree process. STDTT also prepares in-house personnel to effectively assess whether security designs proposed for their sites are compatible with local activity, with personnel resources for assessment, response, and maintenance, and with year-round weather and terrain conditions.

CONTENTS

PREFACE

This report was prepared by Dr. Lindamae Peck, Geophysical Sciences Branch, Cold Regions Research and Engineering Laboratory, U.S. Army Engineer Research and Development Center.

This report, together with the security technology database and the Security Technology Decision Tree Tool, were developed as part of the U.S. Army's Environmental Quality Technology (EQT) Program under the Sustainable Live-Fire Range Design and Maintenance Requirement (2.5 e.). The author thanks James Morse, John Gagnon, and Christopher Williams for their assistance in developing the security technology database. Gary Trachier designed the interview and summary frameworks by which the Security Technology Decision Tree Tool operates, and coded the application.

The author appreciates the helpful technical reviews of Paul Loechl, ERDC-CERL, and Joyce Nagle, ERDC-CRREL.

This report was prepared under the general supervision of Dr. Richard Detsch, Chief, Geophysical Sciences Branch; Lance Hansen, Acting Deputy Director; and James Wuebben, Acting Director, CRREL.

The Commander and Executive Director of the Engineer Research and Development Center is COL James R. Rowen, EN. The Director is Dr. James R. Houston.

Technology for Range Security

LINDAMAE PECK

1 INTRODUCTION

An objective of the U.S. Army's Environmental Quality Technology Program under the Sustainable Live-Fire Range Design and Maintenance Requirement (2.5 e) is to better control access to ranges and training lands through security technology. Issues attributable to unauthorized people on training lands include safety of civilians and soldiers, damage or theft of equipment essential to the training mission, and disruption of training schedules. Potential safety-related problems are injuries to civilians who trespass on training lands for recreational purposes or to scavenge brass, or to soldiers if training equipment or sites are sabotaged. Theft problems include loss of equipment used to operate targets or monitor training activity, as well as removal of artifacts from cultural or historic sites. Damage covers destruction of training equipment and protected sites, including endangered species habitat.

Remote surveillance can detect unauthorized access to ranges and training lands, as well as to isolated cultural sites or endangered species habitats. Remote surveillance encompasses sensor systems for intrusion detection, cameras for assessment of activity, illuminators for day/night assessment capability, and software (automated video surveillance) for evaluation of site imagery.

The effectiveness of surveillance equipment for range security depends on its suitability to the site where it is in use and to the security objectives for that site. Unless on-site personnel have security design experience, the selection, placement, and installation of equipment (sensor systems, cameras, lighting) is likely to be contracted. Even so, in-house personnel must be able to define their security objectives and to assess whether proposed security designs are compatible with local activity, with personnel resources for assessment, response and maintenance, and with year-round weather and terrain conditions. To assist range personnel in their security decisions, the U.S. Army Engineer Research and Development Center, Cold Regions Research and Engineering Laboratory, has developed a Security Technology Decision Tree Tool (STDTT). STDTT is a

computer application that leads the user through specification of security objectives, identification of constraints due to non-interference with mission, and consideration of possible security scenarios, leading to guidance in equipment selection (Peck and Trachier 2004).

The security technology described in this report is not access control equipment. It does not deny access, with the exception of fences and taut wire sensor systems. Such barriers would be ineffective against vehicle assaults; their effectiveness against human intruders would depend on the intruder's willingness to be deterred from trespassing. Instead, the equipment can be used to detect or assess the presence of people in areas that should be unoccupied, and alert designated personnel (e.g., range staff, military police, game wardens) to intruders' presence, thereby increasing the likelihood that the trespassers are stopped and evicted.

2 REMOTE SURVEILLANCE

a. Intrusion detection

Intrusion detection systems (IDSs) are designed to generate alarms when they sense human activity. IDSs attached to a fence (fence-mounted) respond to fence motion caused by someone cutting or climbing the fence. Stand-alone IDSs include thermal infrared, radar, near-infrared beambreak, and taut wire systems. They detect an intruder by sensing, in order, his temperature contrast, his disturbance of a radar field, his interruption of a near-infrared beam, or his displacement of a wire barrier. Buried systems respond either to ground motion caused by the intruder's footsteps or to his disturbance of an above-ground electromagnetic field. Buried IDSs have the advantages of being covert and terrain-following. Taut wire systems provide a barrier as well as detection capability. Radar, thermal (passive) infrared, and beambreak systems represent increasingly narrow detection zones; detection zone width is a consideration when there is little separation between the area being monitored and legitimate activity. Fence-mounted IDSs are easy to install, but have the associated expense of having a fence or other barrier in place. The main classes of intrusion detections systems are described in Appendix A.

A set of IDSs can be used to establish a cordon of detection by having adjoining or overlapping detection zones that completely enclose an area. An individual IDS's alarm directs security personnel to the specific perimeter sector protected by that particular IDS. Alternatively, IDSs might be installed at likely avenues of approach. In this case, an area is monitored for intrusions, not by means of a continuous array of IDSs along its boundary, but by monitoring specific locations at which an intruder would enter that area.

b. Assessment

Cameras provide remote assessment capability. Color and black/white cameras provide useful imagery under natural illumination during daylight hours; color cameras often are preferred because identification of objects is made easier by seeing them in color. Day/night camera units incorporate both a color camera, which is operated during the daytime, and a black/white camera, which is operated at night with either visible or infrared illumination; a day/night camera unit can be set up to switch automatically between the two cameras based on ambient light level. Thermal cameras can be operated day or night without artificial illumination, which avoids the expense (purchase and installation) of lights. Image

intensifiers (night vision devices) are available as stand-alone devices or incorporated in day/night camera units.

None of the cameras is effective under weather conditions that reduce visibility. Color and black/white cameras have reduced range in rain, fog, falling snow, and blowing snow or dust. Black/white cameras also are less effective under overcast conditions that reduce visual contrast in the camera scene. Thermal cameras are less effective when there is little thermal contrast in the scene, particularly when any intruder has the same surface temperature as his background. Image intensifiers are ineffective with high levels of ambient light.

Cameras can be fixed, portable (e.g., mounted to a vehicle), or handheld.

c. Illumination

Hand-held illuminators might be used with portable or handheld cameras that require illumination or by personnel responding to an alarm; they are battery operated. Vehicle-mounted illuminators may operate off the vehicle's battery or have a dedicated battery. Fixed camera installations are more likely to have rigidly mounted illuminators operating on hard power.

d. Automated video surveillance

Automated video surveillance (AVS) equipment performs algorithm-based video motion detection (VMD). Standard VMD relies on changes in pixel gray scale to detect intruder activity, and is subject to numerous nuisance alarms in response to moving shadows, wind-blown vegetation, and birds and animals. Automated surveillance software detects intruders on the basis of their actions and their image configuration, and discriminates against other changes in the camera scene by the characteristic features of those changes. Automated surveillance equipment is more likely than general VMD equipment to generate an acceptably low number of nuisance alarms.

3 SECURITY EQUIPMENT SELECTION PROCESS

Security equipment fulfills its detection, deterrence, or assessment functions only if the equipment is suited both to the site where it is in use and to the security objectives for that site. Unless on-site personnel have security design experience, the selection, placement, and installation of equipment (sensor systems, cameras, lighting) is likely to be contracted. Even so, in-house personnel must be able to define their security objectives and to assess whether proposed security designs are compatible with local activity, with personnel resources for assessment, response, and maintenance, and with year-round weather and terrain conditions.

The Security Technology Decision Tree Tool (STDTT), developed by the U.S. Army Engineer Research and Development Center, Cold Regions Research and Engineering Laboratory, assists users in implementing security measures based on intrusion detection and automated video surveillance technology. STDTT is a computer application that leads the user through specification of security objectives, identification of constraints so that the IDS will not interfere with the mission, and consideration of possible security scenarios, leading to guidance in equipment selection (Peck and Trachier 2004). Even if security design and implementation actually are done by contractors, STDTT will prepare in-house personnel to effectively assess whether proposed security designs and recommended equipment are suited to their security objectives and site conditions.

STDTT counteracts the problem that the use of IDSs lowers the risk level associated with an installation only if the effectiveness of the sensor systems is not jeopardized by errors in their selection, placement, or operation. Vulnerabilities result when terrain, weather, system performance constraints, and detection zone features and maintenance are overlooked or ignored during the planning and implementation of sensor-based physical security. This problem is exacerbated when the users of security equipment have no prior experience with determining what sensor-based scenarios would best meet both their mission and security requirements.

The following sections on IDS, cameras, AVS, and illuminators present some of the factors relevant to selection of these types of security equipment.

a. Intrusion detection systems

Technical information not customarily included in IDS product literature is the IDS's maximum detection distances for a walking person and for a crawling

person, and, perhaps, the recommended maximum detection zone length. Detection distances or detection zone length determine how many IDSs in linear sequence would be required to secure a perimeter. For example, if an area to be monitored for unauthorized access is 600 by 800 m, then using an IDS with a maximum detection zone length of 100 m would require that the perimeter be divided into a minimum of 28 detection zones. These IDS criteria would also determine how wide an avenue of approach could be monitored either with a single IDS or with two opposing IDSs. For example, a freestanding passive infrared (PIR) IDS that typically can detect a walking person to a range of 125 m could be used to monitor an avenue of approach that is 100 m wide; two PIRs facing each other could monitor an avenue of approach that is 200 m wide. In practice, there are factors, such as line-of-sight or changes in boundary orientation, that may limit the extent of a detection zone to less than the maximum possible with a given IDS, and weather conditions can reduce an IDS's effective detection range to less than its physical length.

There is a tradeoff between maximum detection zone length and locating unauthorized access events. Long detection zones are favored from consideration of cost (the longer the detection zone, the fewer the IDSs needed to cover a given distance), while short detection zones more precisely locate an intrusion. The exception is IDSs that locate an intruder within a detection zone; in that case, maximizing the length of the detection zone to reduce the number of IDSs needed does not alter the resolution with which an intrusion is located. In situations where a response force will try to apprehend an intruder, being aware that the unauthorized access occurred between 40 and 50 m from the start of zone A, which is 300 m long, is very useful in directing them where to proceed. Similarly, if the detection zone is under camera coverage, locating an intrusion to within a few meters can selectively direct the camera to the intrusion location and so make it easier for someone viewing the imagery to assess what activity caused the IDS alarm. If response time is too long for precise location of unauthorized access to matter, or if lack of illumination renders cameras useless at night, then being able to locate an intrusion more precisely than by detection zone may not be worthwhile.

b. Cameras

The terms thermal and infrared are often used interchangeably to refer to cameras that image radiation in the 3- to 5-μm or 8- to 12- (or 7- to 14-) μm spectral bands. Such cameras display relative temperature differences among objects being viewed; the relevant camera performance specification is its resolvable temperature difference, i.e., how similar in apparent temperature two

objects can be while still being distinguishable in the camera image. Thermal cameras do not require artificial illumination.

Another option for avoiding the need to provide artificial illumination is a camera system with an image intensifier for nighttime use.

For color and black/white cameras, the relevant performance specifications are the camera's low-light capability (lowest ambient illumination for a useful image with a given lens aperture) and its spectral sensitivity. Relative to black/white cameras, stronger visible illumination and greater sensitivity are needed for color cameras to produce useful imagery. Color cameras have spectral bandwidths of 400 to 790 nm (0.4 to 0.79 μm), which is similar to human eyesight (430 to 690 nm, beyond which limits the eye sensitivity has dropped to 1% of its maximum value). Black/white cameras have extended sensitivity at near-infrared wavelengths, 800 to 1200 nm, and so can be effective at night under moonlight or starlight or when used with near-infrared illuminators. Near-infrared illumination is invisible to humans unless viewed with a night vision device, which is an advantage in applications where visible lighting is unwanted.

c. Automated video surveillance equipment

Automated surveillance equipment is used to analyze imagery (color, black/white, thermal) for activity by humans, vehicles, and animals and for scene changes related to weather events. As a minimum, its features should include selective detection of people and vehicles, discrimination against sources of nuisance alarms (animals, moving shadows, blowing vegetation, etc.), and a means of designating areas of interest (where human or vehicle activity, or both, is to cause alarms) vs. areas where activity is to be ignored. Other features that may be useful in range security applications are a tracking capability, which distinguishes among multiple targets that variously cluster and separate, and a "left object" detection capability, by which an object that enters but does not leave the scene is cause for alarm.

The effectiveness of automated surveillance software is linked to the resolution of the camera that is feeding imagery to the surveillance software. Resolution is expressed in terms of sensor pixels (picture elements per charge-coupled device sensor) or TVL (TV line pairs); TVL can be calculated from pixel count by multiplying the camera's horizontal pixel count by 0.75. Typical camera resolution ranges from 380 to at least 580 TVL for black/white cameras and from 330 to at least 480 TVL for color cameras.

The most significant performance specification for automated surveillance software is the required size of the intruder in the camera scene being analyzed,

i.e., how small can the intruder be in terms of pixels, TVL, or percentage of camera scene, yet still be detected and correctly classified as a potential target rather than a nuisance (e.g., animal or bird). With that information, the necessary combination of camera, lens, and illumination for detecting a specified intrusion (walking person, crawling person, vehicle) at a given range can be determined. Depending on the software, other relevant criteria might be the intruder's direction of movement through the camera scene or the length of time that he remains visible, which would influence camera placement for optimizing detection capability.

d. Illuminators

Round-the-clock assessment capability with color or black/white cameras is possible only if artificial illumination is available to augment natural lighting. Portable (vehicle-mounted and hand-carried) illuminators are relevant to range security as a resource for personnel responding to alarms and for use with temporary camera installations. Permanent or long-term camera installations are more likely to be provided with luminaries mounted to fixed poles.

The main considerations with illuminators are the width of the illuminated field and the range (in the absence of obscurants such as rain, fog, blowing or falling snow, blowing sand) at which the illumination intensity is adequate for discriminating between a human and an animal. Color distortion occurs with some lamps, which would be a concern if identification or apprehension of intruders, using imagery from color cameras, were an objective.

4 SECURITY OPTIONS AND FACTORS

Several options for utilizing security technology to monitor access to training lands are outlined here. These are general applications that are intended to serve as starting points for site-specific decisions on how to meet security objectives at a given installation.

a. Access deterrence

For localized access deterrence, such as at cultural sites or endangered species habitat sites, a taut wire IDS would provide a physical barrier to trespassers as well as detection capability. If site damage is being caused by animals, such as the wild pigs at Ft. Benning or the free-range cattle at Ft. Hood, then a non-lethal electrified version would protect the IDS as well, by discouraging contact. The advantage of a taut wire system over a fence-mounted system is that a separate chain-link fence is not needed. Neither form of a barrier may be acceptable if the protected site is within the active fire portion of a range.

b. Perimeter intrusion detection

The customary form of sensor-based perimeter security at fixed facilities, which is to install a series of IDSs along the entire perimeter, may only rarely be a viable option for range access monitoring because of the size and unimproved condition of training lands. If local security concerns warrant the expense of site preparation, IDS installation, and detection zone maintenance to ensure reliable detection, then the IDSs would be integrated with an alarm annunciator that would be the means of selectively enabling and disabling each IDS zone to avoid alarms during authorized access and egress.

Aside from cost considerations, perimeter intrusion detection may be unacceptable because of the resultant restrictions on where the training land may be accessed by legitimate users. Buried IDSs would not impede access, as personnel and vehicles could freely cross their detection zones; however, it would first have to be determined if buried systems could be placed deep enough to avoid being damaged if driven over by tracked vehicles, yet still maintain an acceptable probability of detecting a human intruder. Free-standing IDSs, such as microwave, near-infrared beam break or passive infrared IDSs, would be more restrictive in that personnel and vehicles could not cross the perimeter in the vicinity of the IDS equipment; based on 100-m-long detection zones, roughly 10% of the perimeter that otherwise might be crossed by vehicles and personnel would be closed to military access. Fences and taut wire systems would limit perimeter

crossings to only those locations where gates or other physical breaks in the fence or taut wire array are placed.

Many freestanding and buried IDSs are relocatable (can be moved from site to site fairly easily) or portable (relocatable, with battery operation and wireless alarm communication), and so could be installed on an emergency basis when warranted by specific military activity on a range or by the current threat level. Such IDSs could be used to establish perimeter security that would restrict military access only while the IDSs were in place, but the recurring burden (time, labor) of deploying the IDSs may be unacceptable. A primary consideration in selecting an IDS for remote locations is how long the IDS can operate on battery power. The major power drain may be the wireless transmission of an alarm alert, rather than intruder sensing. In that case, the type of IDS chosen must have a low nuisance alarm rate under the weather and terrain conditions it will experience; otherwise, the operating period before batteries must be replaced may be unacceptably short.

If IDSs at remote perimeter locations might be subject to vandalism, then another factor in selecting which type of IDS to install is how effectively it can be concealed. The standard IDSs most suited to providing covert perimeter security are buried systems, passive infrared (PIR) systems, and microwave radar systems. When relative ease of installation and detection zone maintenance are considered, then PIRs have the advantage. Among non-standard IDSs are ones that are configured to look like rocks. The suitability of such IDSs for training lands needs to be determined in terms of probability of detection of personnel and vehicles, effective detection range, and required site maintenance. For example, how deep a layer of leaves, snow or windblown soil can accumulate on top of the "rock" before IDS performance is compromised?

Camera coverage of detection zones is necessary for assessment of alarm causes. It would be unrealistic to expect that IDS alarms would be caused solely by human activity, as for a given combination of IDS, terrain, and weather, it is improbable that the IDS would have a zero nuisance alarm rate. To reduce the number of cameras in use, they could be installed at vantage points rather than being collocated with the perimeter IDSs. Pan/tilt cameras or pan/tilt/zoom cameras could be electronically associated with IDS detection zones, such that when an IDS alarms, a camera is automatically directed at its detection zone. Illumination at the detection zones must be adequate for having useful camera imagery.

c. Localized intrusion detection

If natural or man-made features funnel trespassers to certain access points, then localized intrusion detection at choke points would effectively "secure" the

entire perimeter. Portable IDSs are favored for monitoring avenues of approach because they are self-contained in terms of power supply and alarm annunciation. Two considerations with portable IDSs are whether a covert installation is required and whether effective detection capability can be established without obviously modifying the site. Some portable IDSs incorporate a camera and provide for wireless video transmission for remote alarm assessment.

d. Automated video surveillance

Automated video surveillance equipment provides intrusion detection independently of sensor systems. Standard video motion detection is not suitable for monitoring training lands because of its typically high nuisance alarm rate. Object-based motion detection is more likely to be reliable in terms of consistently detecting (and perhaps tracking) human and vehicle movement, while ignoring potential sources of nuisance alarms. If cameras and a means of artificial illumination (other than with thermal cameras) are already in use at a range, then automated surveillance is a relatively easy way to incorporate intrusion detection. The effectiveness of the intrusion detection would depend on whether the camera imagery satisfies the detection criteria of the automated surveillance software (a walking or crawling person is sufficiently large in terms of the image size, moves sufficiently quickly, etc.), whether the intruder employs camouflage or other countermeasures to detection, and whether weather conditions reduce the visible or thermal range of the cameras.

To implement perimeter security with automated surveillance equipment would require having cameras and artificial illumination (other than with thermal cameras) around the perimeter of the training land. The number of cameras would be determined by their effective range (useful viewing distance for human-sized objects). Using a variety of cameras with different effective ranges might permit having some cameras collocated, i.e., several cameras could be mounted on one pole, with one camera/lens combination providing imagery from 5 to 100 m (e.g.), another camera/lens combination providing useful imagery beginning at a distance of ~100 m from the common camera pole, etc. Although cameras might be clustered in one location, artificial illumination has to be provided the entire length of the perimeter if day/night intrusion detection is to be possible.

Because automated video surveillance operates on camera imagery, it also inherently supports alarm assessment, i.e., an observer is presented with the video scene that prompted the AVS to generate an alarm. Identification of the actual activity that caused the AVS to alarm is made easier if the AVS annotates the camera scene with graphics (or some other visual cuing) that direct the ob-

server's attention to the specific portion of the camera scene that was the basis for generating an alarm.

e. Discrimination between humans and animals

Single IDSs capable of distinguishing between humans and animals in their detection zones are ones that respond to magnetic field disturbances. Intruders carrying metal objects should be detected; animals without metal objects would not be detected.

Automated surveillance equipment is capable of distinguishing between humans and animals on the basis of the algorithms in use. Constraints regarding how much of the "intruder" must be visible, especially when moving among trees or through tall brush, need to be known to determine the potential usefulness of automated surveillance in training lands applications. Such constraints can restrict camera placement and selection of the area to be monitored.

IDSs that incorporate both sensors and cameras do not inherently discriminate between humans and animals. Rather, an alarm by the IDS triggers video transmission to a manned station where a person assesses the video and determines whether the intruder is a human or an animal. If the IDS is prone to nuisance alarms caused by naturally occurring changes in its detection zone under the current weather or site conditions, then the person will contend with having to acknowledge many alarms. Artificial illumination is required except with thermal cameras.

It is possible to create a means of possibly distinguishing between humans and animals by using a series of IDSs. One option would be to install portable IDSs at each of three (or more) locations along an avenue of approach. The sequence in which the IDSs alarm (1, 2, 3, vs. 3, 2, 1) indicates direction of motion of the intruder, i.e., entering or exiting the restricted area. The intruder's speed could be estimated from the time interval between alarms by IDSs at known separations. Assuming that an intruder would proceed steadily along the avenue of approach, whereas an animal might browse or move erratically, then the sequence of calculated speeds could indicate, first, whether the alarms were caused by an animal, and second, whether a human intruder was walking or in a vehicle. Interpretation of alarms in this manner would be significantly more complicated, possibly impossible, if there were more than one animal or human intruder, such that each IDS alarmed several times.

Another possibility is to install IDSs, such as portable passive infrared systems, several feet above the ground at what would be chest height of an "average" human. Shorter targets, such as Ft. Benning's wild pigs, would pass under

the IDS's detection zone and so not generate an alarm, but Ft. Hood's free-range cattle would be likely causes of nuisance alarms. In combination with a magnetic IDS, however, even tall animals such as cows or moose might be reliably excluded from causing alarms.

f. Provisions for maintaining high probability of detection and low nuisance alarm rate

Variability in IDS detection capability depends on weather, state of the ground, and groundcover, and on site-specific conditions, such as running water, detection zone exposure to sunlight, or for fence-mounted IDSs, whether the security fence is sheltered or subjected to wind funneling. These factors help determine the probability of detection (P_d) attainable with an IDS without incurring the penalty of a high nuisance alarm rate (NAR). Therefore, diurnal and seasonal variation in site conditions must be considered when selecting IDSs for a site. Diagrams of weather and terrain influences on IDS detection capability (Peck 2002) are presented in Appendix B.

Two IDSs with different sensing technologies can be collocated and operated jointly to reduce both NAR and vulnerabilities arising from site conditions that reduce an individual IDS's P_d. Only if both IDSs detect an intruder would an alarm be generated by the joint system. The combination of IDSs would be based on avoiding overlap in site conditions associated with low P_d and high NAR. The joint IDS can be a single commercial package of two interlinked IDSs, or it can be created on-site through independent installation of two separate IDSs. One of the IDSs could be automated surveillance equipment, provided that the frequency of occurrence and duration of weather-caused episodes of diminished visual or thermal range are acceptable.

g. Additional factors in selection of security equipment

Equipment cost is an obvious consideration when deciding upon a security option . In addition to the cost of a security technology item, such as an IDS, there are associated site-specific costs, as for fencing, camera poles, light poles, luminaries, hard power at IDS and camera locations, video and alarm wiring, site preparation, equipment installation, and detection zone maintenance.

Probability of detection and nuisance alarm rate should be major factors in the selection of IDSs. The difficulty, however, is that P_d and NAR depend on intruder activity, on site conditions, and on how well the IDS is installed and maintained. Regular intrusion trials must be performed to confirm that P_d remains acceptable under ambient conditions and to have early awareness of unacceptable

changes in P_d. Summaries of weather and terrain effects on the P_d and NAR of standard IDSs are presented in Appendix B.

5 SUMMARY AND CONCLUSIONS

Commercial security equipment can support all the scenarios for monitoring training lands that are outlined in the sections, *Security options* and *Discrimination between humans and animals*. Specific products in the categories of IDS, AVS, cameras, and illuminators are represented in a database of security technology compiled for the FY03 range security project and updated in FY05. The database is a mix of current versions of long established security equipment and new, innovative technology. The variety of equipment means that there are many options for monitoring access at training lands without constraining military use of the sites.

STDTT assists a user unfamiliar with security technology in defining his site-specific security objectives, developing surveillance options, and selecting suitable equipment. STDTT operates on the security technology database to extract products that match the requirements developed from the user's decisions as he or she proceeds through the decision tree process. STDTT also prepares in-house personnel to effectively assess whether security designs proposed for their sites are compatible with local activity, with personnel resources for assessment, response, and maintenance, and with year-round weather and terrain conditions.

REFERENCES

Garcia, M.L. (2001) *The Design and Evaluation of Physical Protection Systems.* Boston: Butterworth-Heinemann. 313 p.

Peck, L. (2002) Representation of weather and terrain effects on intrusion detection. In Proc. of the 36th Annual 2002 International Carnahan Conference on Security Technology, 20–24 October, Atlantic City, New Jersey, pp. 179–190.

Peck, L., and G. Trachier (2004) Security technology decision tree tool. In Proc. of the 38th Annual 2004 International Carnahan Conference on Security Technology, 11–14 October, Albuquerque, New Mexico, pp. 91–98.

Ryerson, C.R., and L. Peck (1995). Temporal weather impacts upon exterior intrusion detection systems. U.S. Army Cold Regions Research and Engineering Laboratory, CRREL Report 95-25.

U.S. Navy (1997) *Perimeter Security Sensor Technologies Handbook.* Naval Command, Control and Ocean Surveillance Center, In Service Engineering – East (NISE), North Charleston, South Carolina. Prepared for Defense Advanced Research Projects Agency, Joint Program Steering Group, Arlington, Virginia.

APPENDIX A. CLASSES OF EXTERIOR IDSS

Descriptions of the main classes of exterior intrusion detection systems are presented here.

Acoustic IDSs

Acoustic sensor systems detect vehicles on the basis of the noise generated by them. Acoustic IDSs are not used to detect personnel. An acoustic sensor (microphone) typically is used in a sensor package with a ground motion sensor (geophone). The sensor package reacts first to the geophone signal as a preliminary indication of intruder activity and then, if certain criteria are met, it analyzes the acoustic signal for confirmation that a vehicle is in operation nearby. Joint acoustic/seismic systems typically attempt to identify a detected vehicle as wheeled or tracked, but identification depends on whether the acoustic signature of the vehicle is represented in the system's database. The detection range of an acoustic sensor depends on the propagation of sound between the source and the sensor, which in turn depends on the weather (primarily wind speed profile) and the presence of physical features large enough to block or focus sound waves. If the acoustic sensor activates only after ground motion criteria are met, then weather conditions that impede ground motion can prevent or reduce the likelihood of vehicle detections.

Break Wire IDS

This type of IDS must be in contact with the intruder for an alarm to be generated. The intruder (person or vehicle) physically breaks the tripwire, resulting in an alarm. The extent of the IDS's detection zone is determined by the length of wire in use. The IDS must be manually reset after each break of the wire; there is no detection capability during the period between the wire being broken by an intruder and the IDS being manually reset.

Buried Electromagnetic IDSs

Buried electromagnetic IDSs are commonly referred to as ported coaxial cable (PCC) systems. This type of IDS responds to disturbances to an electromagnetic field set up between two active cables, one that transmits (leaks) electromagnetic energy and one that receives electromagnetic energy; the two cables may be physically separate with a different trench for each, or may be encased together and laid in a single trench. Burial depth is typically 22 cm. Depending on the type of local soil, the narrow trenches may be backfilled entirely with excavated soil, or instead the cables may be placed in a bed of sand with a fill of

local soil on top. The electromagnetic field extends above the ground surface, establishing a volumetric detection zone. Non-intruder disturbances to the field are caused by the motion of surface water or metallic objects. Electromagnetic IDSs in frozen or dry soils have improved detection capability over those in wetter soil. Wet soil in the detection zone may be a persistent condition because of poor drainage, which should be avoided through proper siting of the IDS, or it may occur temporarily during and after rainfall or snowmelt.

Fence-mounted IDSs

This is a broad category of IDSs that are designed to alarm when the security fence to which they are attached is being cut or climbed. They detect a fence disturbance mechanically by means of lost contact when a mass is bounced off its support, electrically by means of a friction-generated charge transfer between the inner and outer portions of a cable attached to the fence (triboelectric), by means of a charge transfer generated in a dielectric within a sensor cable subjected to mechanical stress (piezoelectric), or by means of relative motion between a conductor and a charge-storing dielectric (electret), and optically by changes in the pattern of standing waves of light in optical fiber cables attached to the fence. The characteristics of the fence motion depend on how well the fence posts are anchored in the soil and on the stiffness of the fence panels. The quality of the fence strongly determines the likelihood of nuisance alarms. The dominant environmental cause of fence motion is wind loading. Other sources are the impact of precipitation (falling snow, hail, rain) or of ice or adhered snow that disturbs the fence as it is shed. An intact ice coating on the fence may change the vibration characteristics of the fence panels such that intruder disturbances go undetected.

Ground Motion IDSs

Buried ground motion IDSs are primarily of two types : a liquid-filled tube (pressure tube) or a fiber optic cable. The cable IDS detects ground motion optically by changes in the pattern of standing waves of light in optical fiber cables buried at shallow (~ 5- to 9-cm) depth. A cable is generally laid in a serpentine pattern to give dense coverage, which requires excavation of a wide, shallow trench. It may be attached to plastic construction webbing to give greater coupling to the burial medium, which is typically soil or gravel. If gravel is used, sand may be placed directly on the cable and webbing to protect the cable from abrasion by the gravel. The pressure tube IDS is laid in a linear loop and detects ground motion by changes in the pressure of the enclosed liquid, which varies as the ground deflects under a moving intruder. In both cases, the essential characteristic of the burial medium is that it displaces sufficiently under the intruder's

weight that the induced ground motion meets the alarm criteria of the IDS. Gravel is a favorable burial medium for a ground motion IDS unless, because of poor drainage in winter, the gravel becomes encased in ice. Soil that is wet or loose is favorable; the IDS will have poor detection capability in soil that is frozen or hard packed. Detection capability may be reduced by the presence of a snowcover. Wind-induced motion of surface objects, whose motion couples into the ground, is the primary cause of weather-related nuisance alarms. The detection zone of ground motion IDSs is confined to the area in which the cable or pressure tube is laid; that is, the IDS's detection capability is very localized and generally not wider than the area underlain by the fiber optic cable or the pressure tube.

Magnetic IDSs

Magnetic IDSs detect movement of nearby ferrous metal. They have a short detection range; actual detection range depends on how much ferrous metal is carried by a person or vehicle moving past the sensor. Wildlife, lacking metal objects, would not be expected to activate a magnetic IDS. Consequently, the joint use of a magnetic IDS and another type of IDS is a potential means of discriminating between alarms attributable to human activity and alarms ascribable to wildlife—if both the magnetic IDS and the other IDS alarm, the cause probably is a person or vehicle, as those are the two likely possibilities for having ferrous objects; if only the non-magnetic IDS alarms, the assumption is that the cause of the alarm has no associated ferrous objects, which tends to eliminate people and vehicles. This method of discrimination requires that the intruder (person, vehicle) or wildlife pass close enough to the magnetic IDS that the occurrence or absence of an alarm is significant. The drawback is that many other types of IDSs have substantially longer or wider detection zones than does a magnetic IDS.

Microwave Radar IDSs

There are two types of microwave radar IDSs: bistatic systems that have separate transmitter and receiver units, and monostatic systems that combine the transmit and receive functions in one unit. These IDSs generate an alarm based on the characteristics of a change in the received microwave field, such as would be caused by microwaves scattering off an intruder. An intruder's disturbance to the microwave field is time-varying as he crosses the detection zone, scattering microwaves back toward the transmitting antenna and, for bistatic IDSs, also toward the receiving antenna at the opposite end of the detection zone. Changing site conditions that cause variations in the microwave field, such as reflections

from metal objects or water, are potential causes of nuisance alarms. Vegetation and snow on the ground can shield a crawling intruder from detection.

The received microwave field for bistatic IDSs depends on microwave transmission over the length of the detection zone. One situation that potentially causes nuisance alarms is rapid fluctuations in direct transmission, which can occur during rain and falling snow. The length of the detection zone remains defined by the separation between transmitter and receiver even when there is severe transmission loss. A walking intruder crossing the detection zone close to the receiving unit should still be detected, although the intrusion alarm may occur among nuisance alarms.

The received microwave field for a monostatic microwave IDS is composed of radiation scattered and reflected back to the unit. An intruder crossing the IDS's detection zone alters the microwave field through causing an early return of some microwave radiation and diverting other radiation. For this type of microwave IDS, severe transmission loss in rain or falling wet snow can reduce the effective length of the IDS's detection zone. The stronger the backscatter (return of microwave radiation toward the unit) is, the less the microwaves penetrate through the rain or snow to maintain the extent of detection zone in existence under clear-sky conditions. Nuisance alarms occur when there is variation in the backscattering from rain or airborne snow, such as when the precipitation rate changes during a storm.

Near-infrared Beambreak IDSs

Near-infrared beambreak IDSs are active systems that alarm when a near-infrared beam (between transmitter and receiver units) is interrupted by a sufficient amount for a certain duration. Beambreak sensors located near to the ground, to detect a crawling intruder, are vulnerable to nuisance alarms when snow accumulating on the ground or growing vegetation intrude into the beam. To ensure detection of a crawling intruder, the detection zone should be level, with no elevated areas to shield the intruder or hollows to conceal him. Transmission loss through fog can be a severe problem and limits the maximum zone length for avoidance of fog-related nuisance alarms.

Passive Infrared IDSs

The alarm criteria for passive infrared (PIR) IDSs (also known as thermal infrared systems) generally are the non-uniformity, magnitude, and rate of change of thermal radiance within the detection zone. A thermally uniform background is the ideal situation for thermal infrared IDSs, so snow-covered terrain is favor-

able both for the high probability of detecting an intruder and the low occurrence of nuisance alarms. Daytime nuisance alarms are usually associated with diverse backgrounds having a variety of materials that are alternately sunlit and shaded owing to intermittent cloud cover. As an example, if the detection zone groundcover is a mixture of vegetation and exposed soil, the vegetation and soil will differentially heat and cool under intermittent solar loading, which may result in nuisance alarms from the rapid variation in the thermal radiance received by the PIR. A uniform grass cover is a potential source of daytime nuisance alarms under sunny conditions if the solar-heated grass is long enough to blow in the wind. Regardless of groundcover type, the likelihood of daytime nuisance alarms is low on overcast days or when the IDS's detection zone is shaded.

Seismic IDSs

Seismic sensors are point sensors that detect ground motion. Their detection range is greater for a moving vehicle than for a moving person. Seismic sensors are omnidirectional, which generally renders them inappropriate for situations where legitimate activity is ongoing near the area being monitored for intruders. In such situations the seismic sensor does not discriminate between ground motion generated by the legitimate activity and ground motion generated by an approaching intruder. Seismic sensors are best used in remote areas where any human- or vehicle-generated ground motion is significant. Similarly, they may be unreliable where there is significant ground motion caused by nearby traffic, pedestrians, or vibrating equipment that overwhelms the sensor or causes nonintruder alarms. Seismic detection of humans can be unreliable if the ground is frozen or it is snow covered, with the snow cover being rigid enough to support the intruder's weight. The primary cause of weather-related nuisance alarms is wind-induced motion of surface objects that couples into the ground. Buried fiber optic cable IDSs and buried pressure tube IDSs also detect ground motion induced by an intruder, but their detection range by design is little more than the width of the area in which the line sensor is laid.

Taut Wire IDSs

Taut wire IDSs alarm at the displacement of a strand of wire under tension. This IDS is installed as a physical barrier consisting of a vertical array of wires (parallel to the ground) with perhaps additional wires on angled outriggers. Only a few centimeters of vertical clearance separate two wires or separate the bottom wire and either the ground surface or the top of a wall or fence. An intruder cannot pass his body through the gap without deflecting one or two adjacent wires. Icing and snow accumulation on the wires are potential problems; their severity

depends on the collection efficiency of the wire (barbed wire has a higher collection efficiency than smooth wire has) and on the weather conditions.

Video Motion Detection Systems and Automated Video Surveillance Systems

Standard video motion detection (VMD) relies on changes in pixel gray scale to detect intruder activity, and is subject to numerous nuisance alarms in response to moving shadows, wind-blown vegetation, and birds and animals. Automated video surveillance (AVS) software detects intruders on the basis of their actions and their image configuration, and discriminates against other changes in the camera scene by the characteristic features of those changes. Automated video surveillance equipment is more likely than general VMD equipment to generate an acceptably low number of nuisance alarms. Detection capability with VMD and AVS is diminished by precipitation and fog (decreased visibility, loss of visual contrast) and by low visual contrast (diffuse illumination under cloud cover). High levels of direct or reflected solar radiation may saturate the camera detector, rendering the IDS ineffective.

APPENDIX B. WEATHER AND TERRAIN DIAGRAMS FOR INTRUSION DETECTION SYSTEMS

Weather and terrain diagrams (Peck 2002) are presented for eight classes of exterior IDSs: passive (thermal) infrared, fence-mounted, microwave radar, taut wire, near-infrared beambreak, ground motion, ported coaxial cable, and video motion detection. The diagrams indicate interactions among site conditions and their joint impact on IDS detection capability, i.e., which combinations of conditions are compatible with operating an IDS at a high sensitivity (which generally equates to a high P_d) while maintaining a low NAR. Several of the diagrams also highlight specific changes in P_d with site conditions.

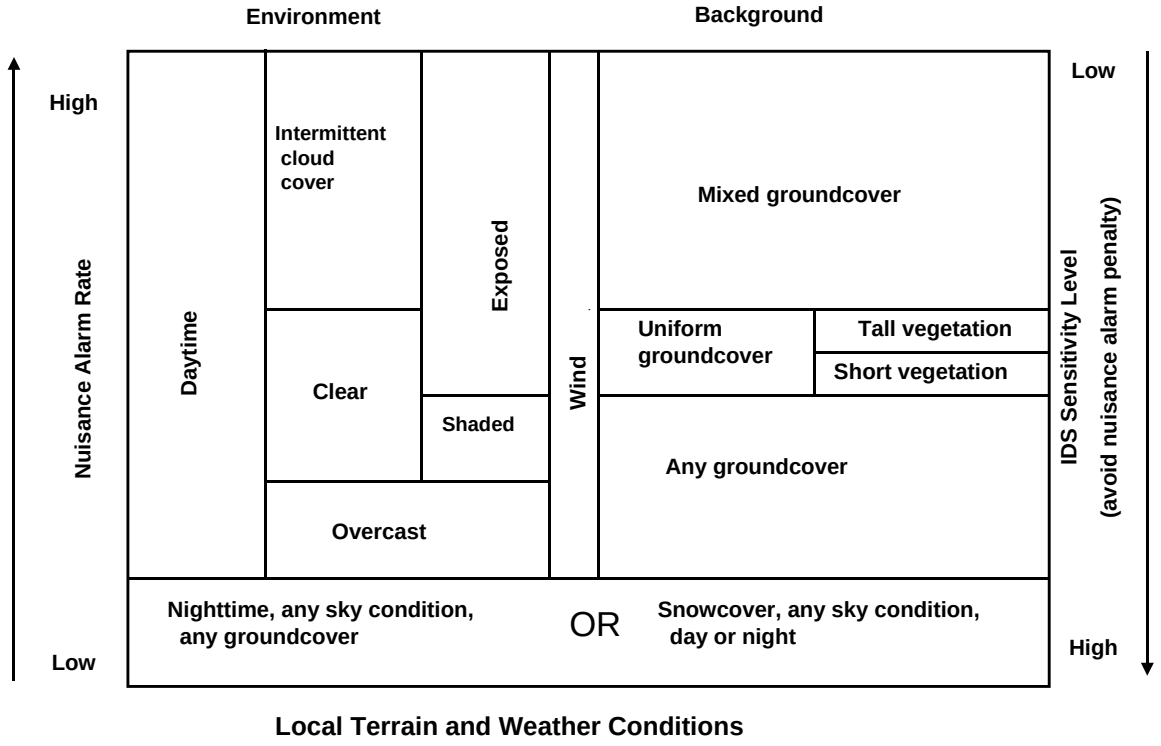

Figure B1. Weather and terrain influences on passive (thermal) infrared IDSs, showing the tradeoff between IDS sensitivity setting and occurrence of environment-related nuisance alarms.

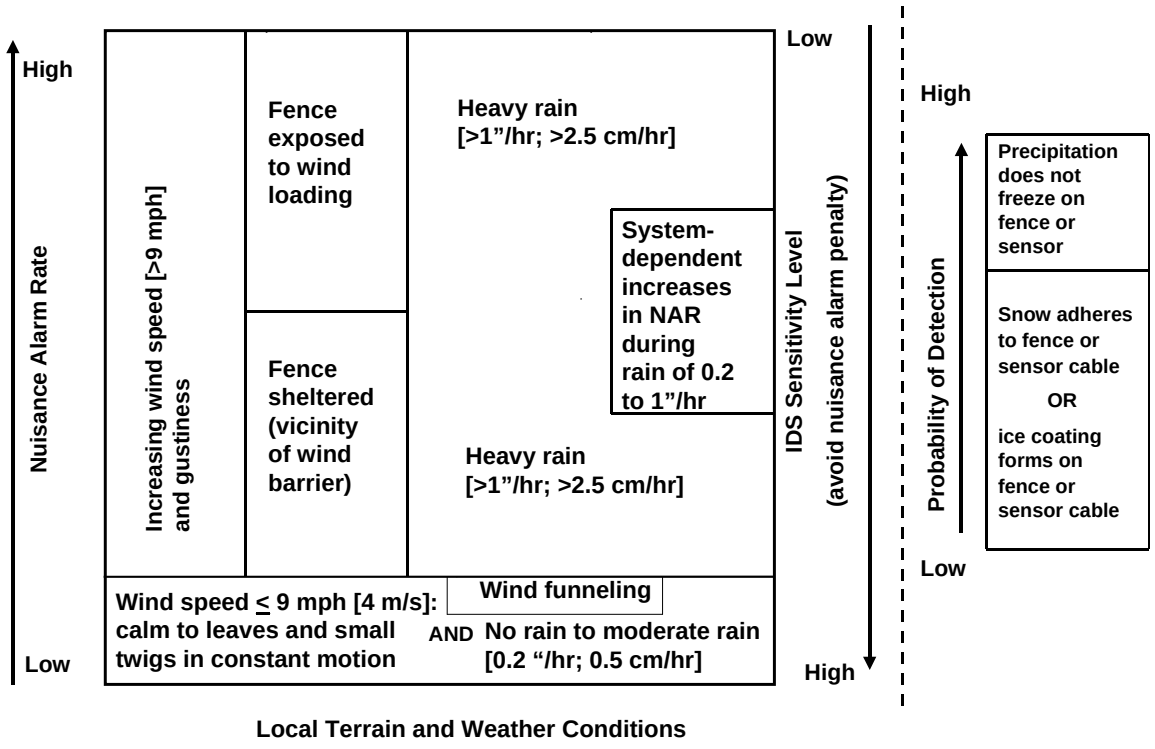

Figure B2. Weather and terrain influences on fence-mounted IDSs, showing (left) the tradeoff between IDS sensitivity setting and occurrence of environment-related nuisance alarms, and (right) the effect of frozen precipitation on probability of detection.

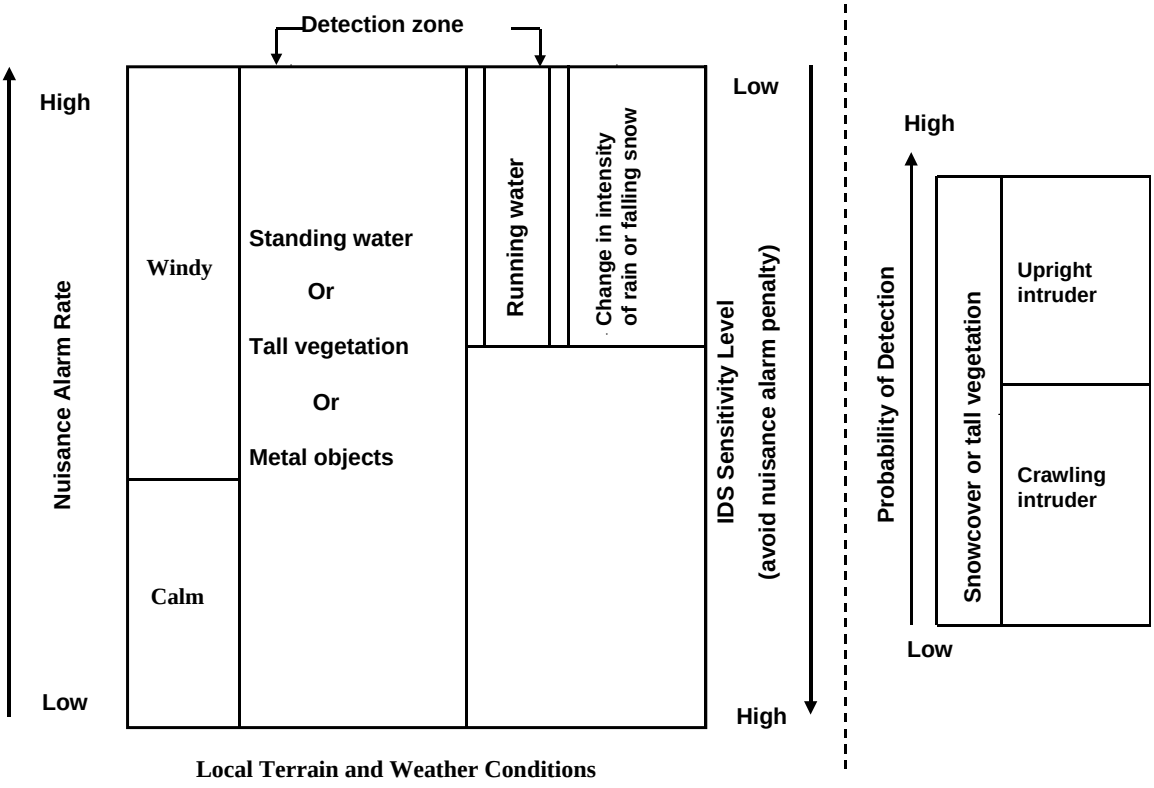

Figure B3. Weather and terrain influences on microwave radar IDSs, showing (left) the tradeoff between IDS sensitivity setting and occurrence of environment-related nuisance alarms, and (right) the effect of intruder concealment on probability of detection.

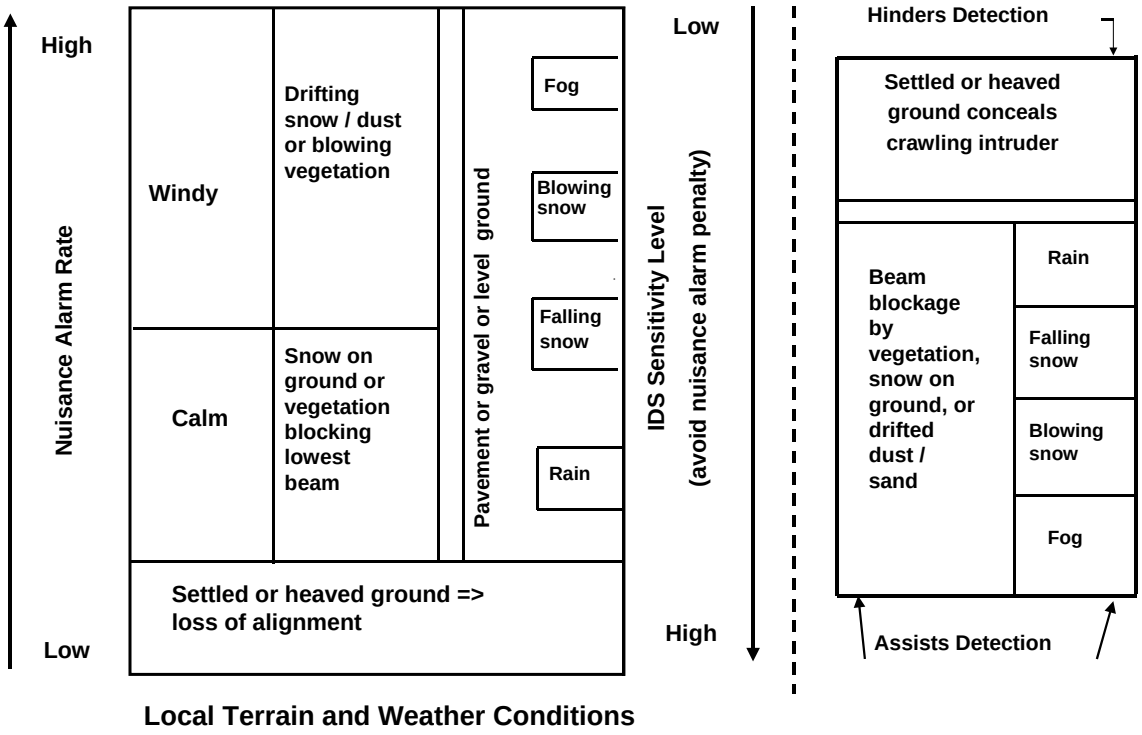

Figure B4. Weather and terrain influences on near-infrared beambreak IDSs, showing (left) the tradeoff between IDS sensitivity setting and occurrence of environment-related nuisance alarms, and (right) the effect of pre-existing beam blockage on intruder detection.

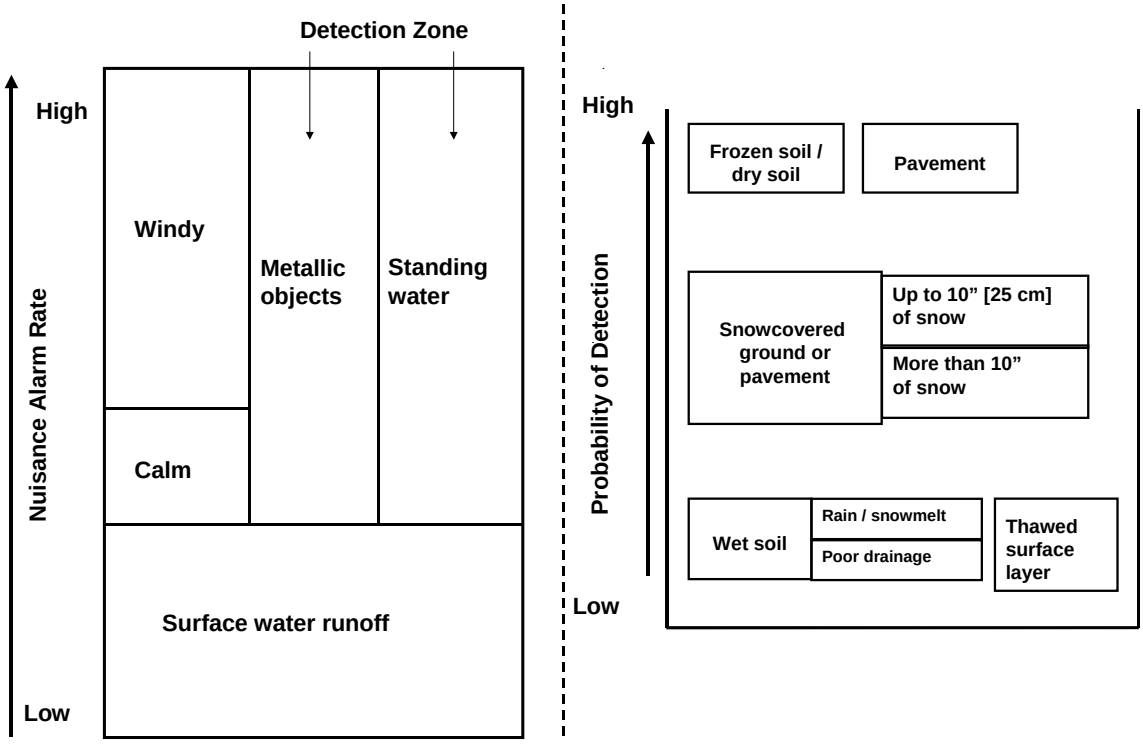

Figure B5. Weather and terrain influences on buried ported coaxial cable IDSs, showing (left) the relative severity of site conditions relative to environment-related nuisance alarms, and (right) the effects of ground state and snowcover on probability of detection.

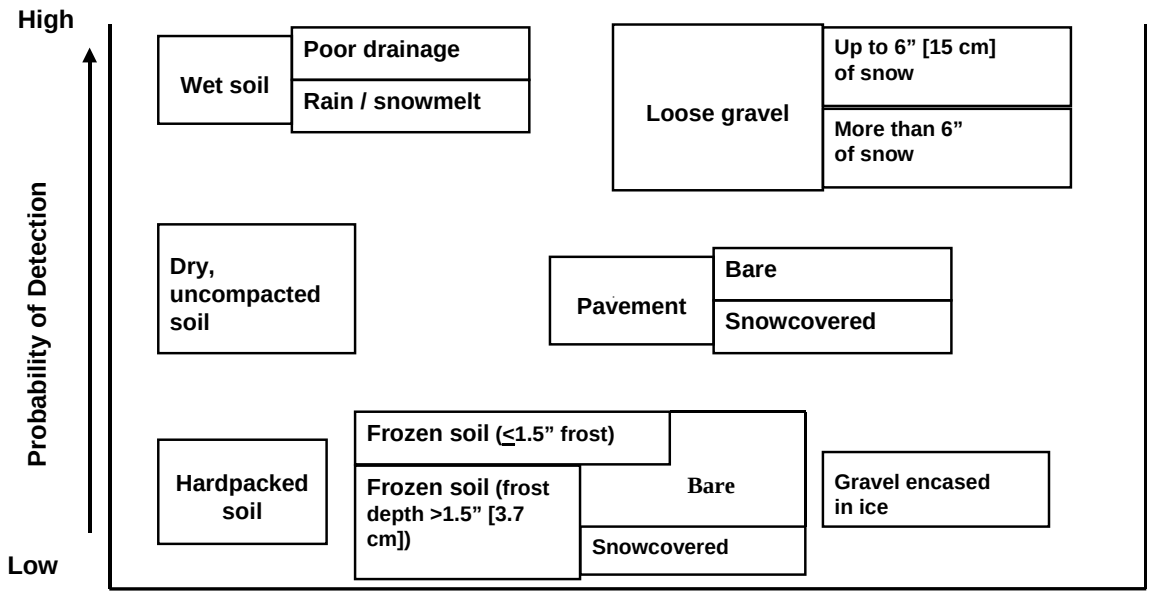

Figure B6. Weather and terrain influences on probability of detection with ground motion IDSs.

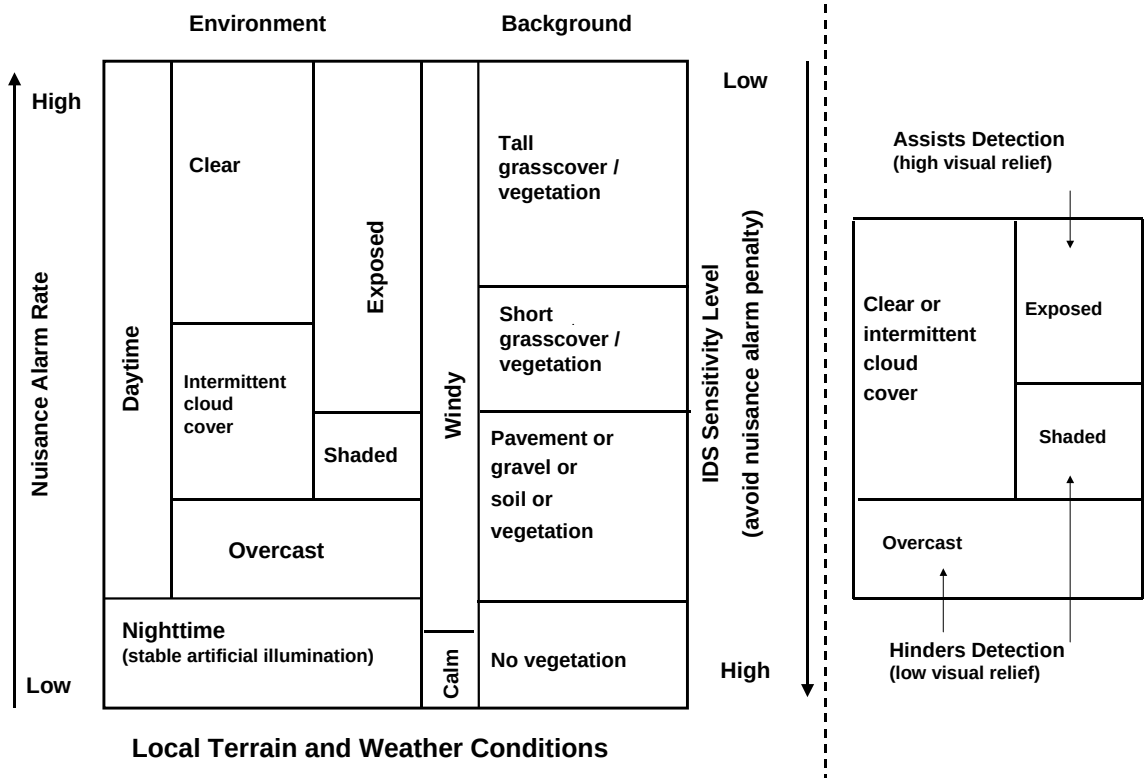

Figure B7. Weather and terrain influences on video motion detection IDSs, showing (left) the tradeoff between IDS sensitivity setting and occurrence of environment-related nuisance alarms, and (right) the effect of visual relief on intruder detection.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
June 2005		

4. TITLE AND SUBTITLE

Technology for Range Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lindamae Peck

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Cold Regions Research and Engineering Laboratory
72 Lyme Road
Hanover, NH 03755-1290

8. PERFORMING ORGANIZATION REPORT NUMBER

ERDC/CRREL TR-05-11

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army Environmental Center
Aberdeen Proving Ground, MD 21010-5401

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Commercial security equipment can support all the scenarios for monitoring training lands that are outlined in the sections, *Security options* and *Discrimination between humans and animals*. Specific products in the categories of intrusion detection systems, automated video surveillance, cameras, and illuminators are represented in a database of security technology. The database is a mix of current versions of long established security equipment and new, innovative technology. The variety of equipment means that there are many options for monitoring access at training lands without constraining military use of the sites. The Security Technology Decision Tree Tool (STDTT) assists a user unfamiliar with security technology in defining his site-specific security objectives, developing surveillance options, and selecting suitable equipment. STDTT operates on the security technology database to extract products that match the requirements developed from the user's decisions as he or she proceeds through the decision tree process. STDTT also prepares in-house personnel to effectively assess whether security designs proposed for their sites are compatible with local activity, with personnel resources for assessment, response, and maintenance, and with year-round weather and terrain conditions.

15. SUBJECT TERMS

Intrusion detection systems
Physical security
Range security
Security technology
Training lands security

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
Unclassified	Unclassified	Unclassified	Unclassified	37	